UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/036,128	12/26/2001	David C. Collier	214	3434

31665 7590 11/01/2006

PATENT DEPARTMENT
MACROVISION CORPORATION
2830 DE LA CRUZ BLVD.
SANTA CLARA, CA 95050

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 11/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/036,128	COLLIER ET AL.	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 October 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11,19,24-35,37-56 and 66-72* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11,19,24-35,37-56 and 66-72* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This application has been abandoned on 12/20/2005, applicant has been filed Petition for Revival under CFR 1.137(b) on 01/19/2006, and the request for Petition for Revival has been granted on 08/25/2006. Accordingly, applicant's amendments/arguments are moot in view of new grounds of rejection and the action has been made final.

2. Applicant amends all independent claims 1 and 42, and dependent claims 19, 24-33, and 66-69, cancels claims 12-18, 20-23, 36, and 57-65, and claims 1-11, 19, 24-35, and 37-56, and 66-72 are pending.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-11, 19, 24-35, and 37-56, and 66-72 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kori (Patent No.: US 2001/0053979 A1) in view of Bestock et al. USPN 4,933,971.

Regarding claim 1, Kori discloses an apparatus for accessing material, comprising:

a secure registry encrypted with a registry key (0034, fig. 3A and fig. 11) that was generated by using an identification of an authorized entity (0056; *kc is created using user's*

password identifier), storing another key useful for decrypting material (fig. 11; *stored encrypting key*); and

decrypt said secure registry using a registry key for retrieval of said another key (0082).

Kori fails to disclose a control module configured to regenerate said registry key by using an identification of a current entity associated with said secure registry at the time of said regeneration, and decrypt using said regenerated registry key, and provided identifications of said authorized and current entities are the same.

However, Bestock et al. discloses a method of encrypting and decrypting data by **periodically** generating a unique dynamic encryption key using same system **seed key/identifier** residing only in the host computer (col. 4 lines 8-16, and col. 8 lines 31-44), that is a key is generated in a predetermined time using same seed key of host computer/current entity associated with host computer secure registry initial value/seed at the time of regeneration (claims 3 and 10, and col. 8 lines 31-44) and decrypting communication using the periodically regenerated key (col. 4 lines 38-40 and fig. 5), wherein the seed key remains the same each time the key is generated in a predetermined time (claims 3 and 10, col. 10 lines 30-col. 11 lines 16, and col. 8 lines 31-44).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Bestock et al. with in the system of Kori because they are analogous in data encryption and data security. One would have been motivated to incorporate the teachings of Bestock et al. within the system of Kori because it would secure the data protection system by regenerating a key from the same seed identifier and/or if the key

is regenerated from unknown seed identifier the system would not allow a decryption access to the data and further enhance data/copy protection security.

As per claims 2, 7, and 43, Kori further teaches the apparatus, wherein said control module receives said material as streaming media, and is further configured to decrypt said material using said another key (Kori page 2 par. 0028, page 5 par. 0082, and par. [0086-0088]).

As per claims 3, 8, 44, and 51 Kori further teaches the apparatus, wherein said streaming media/file is in MPEG-4 format encrypted with at least one content key, and said control module receives said at least one content key encrypted with said another key (0033).

As per claims 4, 9, 46, and 53, Kori further teaches the apparatus, wherein said another key comprises at least one license key corresponding to a license to use said material (Kori fig. 11, 0034, 0082; encrypting key).

As per claims 5, 10, 47, and 54 Kori teaches the apparatus, wherein said streaming media/file is in MPEG-4 format encrypted with at least one content key, and said control module receives said at least one content key encrypted with a public key of said apparatus (Kori page 5 par. 0081).

As per claims 6 and 11, Kori further teaches the apparatus, wherein said another key comprises a private key of said apparatus (Kori page 5 par. [0080-0081]).

As per claim 19 Kori further teaches the apparatus, wherein said sensed entity identification is unique for said apparatus (col. 4 lines 7-14; *seed key of the host system is unique to the host and only disclosed in the host to generate periodic key in a time interval*).

As per claim 24, Bestock et al. teaches the apparatus, wherein said identification of said current entity is a computer identification (claim 1(c)).

As per claim 25, Kori and Bestock et al. teach all the subject matter as described above. In addition, 3qa3qaak teaches the apparatus, wherein said identification of said current entity is a network interface card identification (the Examiner takes an official notice on wherein said ID of the current entity is a network interface card (NIC) ID because it would be obvious to one ordinary skill in the art at the time of the invention was made to employ the system of computer identification seed with network interface card identification in order to use network interface card ID unique seed because identifier is just a binary seed and would identify and work for NIC).

As per claim 26, Bestock et al. further teaches the apparatus, wherein said identification of said current entity is a hard disk drive identification (col. 8 lines 30-col. 11 lines 7).

As per claim 27, Bestock et al. teaches the apparatus, wherein said identification of current entity is unique for a hardware device connectable to said apparatus (abstract).

As per claim 28, Kori and Bestock et al. teach all the subject matter as described above. The apparatus, wherein said identification of current entity is a smartcard identification (the Examiner takes an official notice on wherein said identification of current entity is unique for a hardware device connectable to said apparatus because it would be obvious to one ordinary skill in the art at the time of the invention was made to employ the system of computer identification seed with smart card identification in order to use smart card's unique seed because identifier is just a binary seed and would identify and work for smart card).

As per claim 29, Kori and Bestock et al. teach all the subject matter as described above. The apparatus, wherein said sensed entity identification is a content storage unit identification (the Examiner takes an official notice on wherein said sensed entity identification is a content storage unit identification because it would be obvious to one ordinary skill in the art at the time of the invention was made to employ the system of computer identification seed with storage unit identification in order to use storage unit's unique seed because identifier is just a binary seed and would identify storage unit).

Regarding claims 30 and 68 Bestock et al. further discloses the apparatus wherein said identification of said current entity is unique to a user of said apparatus (col. 4 lines 30-32)

As per claim 31, Kori and Bestock et al. teach the apparatus, wherein said sensed entity identification is a credit card number (the Examiner takes an official notice on wherein said

sensed entity identification is a credit card number because it would be obvious to one ordinary skill in the art at the time of the invention was made to modify the system of computer identification seed with credit card number in order to use credit card number as a seed because credit card number is an identifier and identifier is just a binary seed and would identify an entity).

As per claim 32, Kori further teaches the apparatus, wherein said identification said current entity is a predefined user identification (0060-0061).

As per claims 33-35 and 71, Kori and Bestock et al. discloses all the subject matter. The examiner takes an official notice on wherein said identification of said current entity is a biometrics/fingerprint/speech based identification (because it would be obvious to one ordinary skill in the art at the time of the invention was made to modify the system of computer identification seed with biometrics identification in order to use biometrics identification as a seed because biometrics identification is an identifier and identifier is just a binary seed and would uniquely identify an entity see Novak page 7 par. 103 and page 6 par. 0089.

As per claim 37, Kori further teaches the apparatus, wherein said control module comprises a processor and a control program running on said processor (Kori fig. 8 No. 11).

As per claim 38, Kori further teaches the apparatus, wherein said control module includes logic circuitry (0066).

As per claim 39, Kori further teaches the apparatus, wherein said control module is license-enabled to a unique identification of said apparatus (0060-0061).

As per claim 40, Kori further teaches the apparatus, wherein said secure registry further stores information related to said material (Kori fig. 11; audio/video data).

As per claim 41, Kori teaches the apparatus, wherein said information related to said material includes usage rights included in a license for said material (Kori fig. 3A, and page 2 par. 0034, and fig. 11).

As per claim 42, Kori teaches a method for accessing material, comprising:

receiving (0082) a secure registry that has been encrypted with a registry key (0034, fig. 3A and fig. 11) that was generated by using identification of an authorized entity (0056; *kc is created using user's password identifier*);

decrypting said secure registry with a registry key (0082);

retrieving another key from said decrypted secure registry (fig. 13, and 0082) decrypting encrypted material using said another key to access said material (Kori Fig. 13, and page 5 par. 0082).

Kori fails to disclose regenerating said registry key using an identification of an entity associated with said secure registry at the time of said regeneration, and decrypting using regenerated key.

However, Bestock et al. discloses a method of encrypting and decrypting data by **periodically** generating a unique dynamic encryption key using same system **seed key/identifier** residing only in the host computer (col. 4 lines 8-16, and col. 8 lines 31-44), that is a key is generated in a predetermined time using same seed key of host computer/current entity associated with host computer secure registry initial value/seed at the time of regeneration (claims 3 and 10, and col. 8 lines 31-44) and decrypting communication using the periodically regenerated key (col. 4 lines 38-40 and fig. 5).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Bestock et al. with in the system of Kori because they are analogous in data encryption and data security. One would have been motivated to incorporate the teachings of Bestock et al. within the system of Kori because it would secure the data protection system by regenerating a key from the same seed identifier and/or if the key is regenerated from unknown seed identifier the system would not allow a decryption access to the data and further enhance data/copy protection security.

As per claim 45, Kori teaches the method, wherein said decrypting encrypted material using said another key to access said material, comprises:

decrypting said at least one content key with said another key (Kori page 5 par. 0082); and

decrypting said encrypted material with said at least one content key to access said material (Kori page 5 par. 0082).

As per claims 48, and 55, Kori teaches the method, wherein said another key comprises a private key of said recipient of said material (Kori page 5 par. 0081-0082).

As per claims 49 and 56, Kori teaches the method, wherein said decrypting encrypted material using said another key to access said material, comprises:

decrypting said at least one content key with said private key (kori page 5 par. 0081-0082); and

decrypting said encrypted material with said at least one content key to access said material (kori page 5 par. 0081-0082).

As per claim 50, Kori teaches the method, further comprising receiving said encrypted material as a file (Kori page 5 par. 0086-0088).

As per claim 52, Kori teaches the method, wherein said decrypting encrypted material using said another key to access said material, comprises:

decrypting said at least one content key with said another key (Kori page 5 par. 0081-0082); and

decrypting said encrypted material with said at least one content key to access said material (Kori page 5 par. 0081-0082).

As per claim 66, Bestock et al. teaches the method, wherein said identification of said entity is unique to a host (col. 4 lines 7-14).

As per claim 67, Kori and Bestock teach all the subject matter as described above. In addition, both teach the apparatus, wherein said identification of said entity is unique for a hardware device connectable to said apparatus (Kori 000056, and 0060-0061, and Bestock et al. col. 4 lines 7-14).

As per claim 69, Kori further teaches the method, further comprising receiving said sensed entity identification from information entered into an input device by said user (0060-0061).

As per claim 70, Kori teaches the method, wherein said input device is a keyboard (Kori page 2 par. 0028, and fig. 3a & 3b).

As per claim 72, Kori teaches the method, further comprising after said decrypted encrypted material using said another key to access said material:

using said material according to a license stored in said secure registry along with said another key (Kori page 5 par. 0081-0082).

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

E.S.
October 27, 2006

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

10/29/06